APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/378,226	08/19/1999	MARK D. RIGGINS	40827.00011	8867

30256   7590   10/04/2003

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2131	12

DATE MAILED: 10/04/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)	
Office Action Summary	09/378,226	RIGGINS, MARK D.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 June 2003</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-30</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-30</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>19 August 1999</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>3-11</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

Drawings

1. The drawings are objected for the reasons stated in PTO-948. A proposed drawing correction

or corrected drawings are required in reply to the Office action to avoid abandonment of the

application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
> subject matter which the applicant regards as his invention.

2. Claims 19 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being

incomplete for omitting essential steps, such omission amounting to a gap between the

steps. See MPEP § 2172.01.

The omitted steps are: steps for "deriving a key". The applicant recites "sending a

decryption downloadable for deriving a key from a password and a hint". However, there are no

steps recited in how the key is actually derived. Additionally, there is no end result to both

claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on
> sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-18 and 21-30 are rejected under 35 U.S.C. 102(b) as being anticipated by

Kaufman et al U.S. Patent No. 5,491,752.

As to claims 1 and 8, Kaufman et al discloses obtaining a hint [column 6, lines 63-66]. Kaufman et al discloses obtaining a password [column 6 line 66 to column 7 line 1]. Kaufman et al discloses performing a hashing algorithm on the hint and the password to generate a key [column 7, lines 2-5]. Kaufman et al discloses encrypting data using the key [column 7, lines 18-22]. Kaufman et al suggests sending the encrypted data to a server for storage [column 11, lines 44-55].

As to claim 2, Kaufman et al discloses that the step of performing a hashing algorithm includes hashing the password [column 7, lines 2-5].

As to claim 3, Kaufman et al discloses that the step of performing a hashing algorithm includes hashing the password to derive a first secret [column 10, lines 6-17], hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key [column 11, lines 26-55].

As to claim 4, Kaufman et al discloses a user interface for obtaining a password [figure 5,]. Kaufman et al discloses a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key [column 7, lines 2-5]. Kaufman et al discloses an encryption engine coupled to the key generator for encrypting data using the key [column 7, lines 18-22]. Kaufman et al discloses a communications module coupled to the engine for sending the encrypted data to a server for storage [figure 5].

As to claim 5, Kaufman et al discloses a hint generator for generating the hint [figure 5].

As to claim 6, Kaufman et al discloses that the key generator hashes the password [figure 5].

As to claim 7, Kaufman et al discloses that the key generator hashes the password to derive a first secret [column 10, lines 6-17], hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key [column 11, lines 26-55].

As to claim 9, Kaufman et al discloses that the system includes code stored on a computer-readable storage medium [figure 5].

As to claim 10, Kaufman et al suggests that the system includes code embodied in a carrier wave [figure 5].

As to claim 11, Kaufman et al suggests receiving a request to store encrypted data from a client [column 1, lines 36-45]. Kaufman et al discloses sending an encryption downloadable for deriving a key to encrypt data to the client [column 12, lines 37-40]]. Kaufman et al teaches receiving encrypted data that was encrypted by the encryption downloadable from the client [column 11, lines 43-54]. Kaufman et al discloses obtaining a hint corresponding to the encrypted data and needed for regenerating the key and storing the hint and the encrypted data [column 12, lines 37-63].

As to claim 12, Kaufman et al discloses an encryption downloadable for deriving an encryption key from a password and a hint [column 7, lines 2-5]. Kaufman et al suggests a web server for interfacing with a client for sending the encryption downloadable to the client [column 11, lines 44-55]. Kaufman et al discloses receiving encrypted data that was encrypted by the encryption downloadable from the client [column 11, lines 43-54]. Kaufman et al suggests memory coupled to the web server for storing a hint corresponding to the encrypted data and needed to regenerate the key from the client and the encrypted data [column 7, lines 2-5].

As to claims 13 and 16, Kaufman et al discloses obtaining a password [column 6 line 66 to column 7 line 1]. Kaufman et al discloses receiving encrypted data and a hint corresponding to the encrypted data from a server [figure 6]. Kaufman et al discloses performing a hashing algorithm on the password and the hint to generate a key for decrypting the encrypted data [figure 6].

As to claim 14, Kaufman et al discloses that the step of performing a hashing algorithm includes hashing the password [column 9, lines 41-60].

As to claim 15, Kaufman et al discloses a user interface for obtaining a password [column 6 line 66 to column 7 line 1]. Kaufman et al discloses a communications module for receiving the encrypted data and a hint corresponding to the encrypted data from a server [figure 6]. Kaufman et al discloses a key generator for performing a hashing algorithm on the password and the hint to generate a key for decrypting the encrypted data [column 9, lines 41-60].

As to claim 17, Kaufman et al discloses that the system includes code stored on a computer-readable storage medium [figure 5].

As to claim 18, Kaufman et al suggests that the system includes code embodied in a carrier wave [figure 5.

As to claim 21, Kaufman et al discloses obtaining a password [column 6 line 66 to column 7 line 1]. Kaufman et al discloses deriving a first secret from the password [column 10, lines 6-17]. Kaufman et al discloses receiving a hint corresponding to data to be decrypted from a server [figure 6]. Kaufman et al discloses deriving an intermediate index from the first secret and the hint [figure 6]. Kaufman et al discloses sending the intermediate index to the server [figure 6].

As to claim 22, Kaufman et al discloses that deriving the first secret includes hashing the password [column 10, lines 6-17].

As to claim 23, Kaufman et al discloses that deriving an intermediate index includes hashing the first secret and the hint [column 7, lines 2-5].

As to claim 24, Kaufman et al discloses a user interface for obtaining a password [column 6 line 66 to column 7 line 1]. Kaufman et al discloses an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password [figure 5]. Kaufman et al discloses a communications engine coupled to the index generator for sending the intermediate index to the server [figure 5].

As to claim 25, Kaufman et al discloses that the index generator generate the intermediate index by hashing the hint and the secret [column 9, lines 41-60].

As to claim 26, Kaufman et al discloses means for obtaining a password [column 6 line 66 to column 7 line 1]. Kaufman et al discloses means for deriving a first secret from the password [column 9, lines 41-60]. Kaufman et al discloses means for receiving a hint corresponding to data to be decrypted from a server [figure 6]. Kaufman et al discloses means for deriving an intermediate index from the first secret and the hint [column 9, lines 41-60]. Kaufman et al discloses means for sending the intermediate index to the server [figure 6].

As to claim 27, Kaufman et al discloses that the system includes code stored on a computer-readable storage medium [figure 5].

As to claim 28, Kaufman et al suggests that the system includes code embodied in a carrier wave [figure 5].

As to claim 29, Kaufman et al discloses receiving an indication of encrypted data to be decrypted [figure 6]. Kaufman et al discloses transmitting to a client a hint corresponding to the indication [figure 6]. Kaufman et al discloses a decryption downloadable for deriving an intermediate index from a password and the hint. Kaufman et al discloses receiving the intermediate index from the client. Kaufman et al discloses deriving a decryption key from a second secret corresponding to the user and the intermediate index.

As to claim 30, Kaufman et al discloses a second secret corresponding to a user. Kaufman et al discloses a decryption downloadable for generating an intermediate index from a password and a hint [column 7, lines 2-5]. Kaufman et al suggests a web server for receiving an indication of encrypted data to be decrypted [column 11 line 56 to column 12 line 7]. Kaufman et al discloses transmitting the decryption downloadable and a hint corresponding to the indication to a client [figure 6]. Kaufman et al discloses receiving an intermediate index from the client [figure 6]. Kaufman et al discloses a server-resident module for deriving a key for decrypting the encrypted data from the second secret and the intermediate index [figure 6].

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy
September 10, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100